IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.	:	09/898,365
Applicants	:	Poo, Teng Pin and Lim, Lay Chuan
Filed	:	July 3, 2001
Art Unit	:	2133
Examiner	:	Gelagay, Shewaye
Confirm. No.	:	4356
Docket No.	:	1601457-0007
Customer No.	:	007470

Mail Stop **Appeal Brief – Patents**
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certificate of Transmission

I hereby certify that this paper is being transmitted to the U.S. Patent and Trademark Office via the Electronic Filing System in accordance with 37 C.F.R. § 1.6(a)(4) on the date indicated below.

Date: 3/20/08

By: Gail Ohlsson
Gail Ohlsson

APPEAL BRIEF

This is an appeal pursuant to 37 C.F.R. § 41.37 from the decision of the Examiner in the above-identified application as set forth in the Office Action dated February 20, 2007. The rejected claims are reproduced in Appendix A. A Notice of Appeal was filed on August 20, 2007.

The fee of $500.00 for filing an Appeal Brief (Large Entity) pursuant to 37 C.F.R. § 41.20(b)(2) has previously been paid with an earlier appeal brief. A Petition for the five-month extension of time is enclosed herewith along with the fee of $2,230.00 (Large Entity). Any additional fees or charges in connection with this application may be charged to White & Case Deposit Account No. 50-3672.

REAL PARTY IN INTEREST

The assignee, Trek Technology (Singapore) Pte. Ltd., of applicant(s), Teng Pin Poo and Lay Chuan Lim, is the real party of interest in the above-identified U.S. Patent Application.

RELATED APPEALS AND INTERFERENCES

There are no other appeals and/or interferences related to the above-identified application at the present time.

STATUS OF CLAIMS

Claims 15 and 21 have been cancelled. Claims 1-14, 16-20 and 22-24 have been rejected. Claims 1-14, 16-20, and 22-24 are on appeal.

STATUS OF AMENDMENTS

In the paper mailed by Applicant on February 24, 2006, Applicant submitted proposed claim amendments for claims 3 and 9. In the Advisory Action mailed on March 15, 2006, the Office indicated that the proposed amendments will be entered for the purposes of appeal only.

SUMMARY OF CLAIMED SUBJECT MATTER

Independent Claims 1, 7 and 17

Appellant's invention is directed to a portable data storage device having biometrics-based authentication capabilities so the device can authenticate users before granting access to the data storage capabilities of the device. As illustrated in Figure 1B and Figure 2 of the application, reproduced below, portable device 170 has a housing, within which is housed a microprocessor 111 and a biometrics-based authentication module 150 controlled by the microprocessor 111, and may have volatile memory 116 and/or non-volatile memory 117 as well as a biometrics sensor 152. *See* Specification page 8, lines 23-27; page 9, lines 7-8 and 15-18. Portable device 170 also includes a USB plug 118 which is integrated into its housing and which is directly coupled to a USB host controller 193 of a host platform. *See* Specification page 8, lines 2-5.

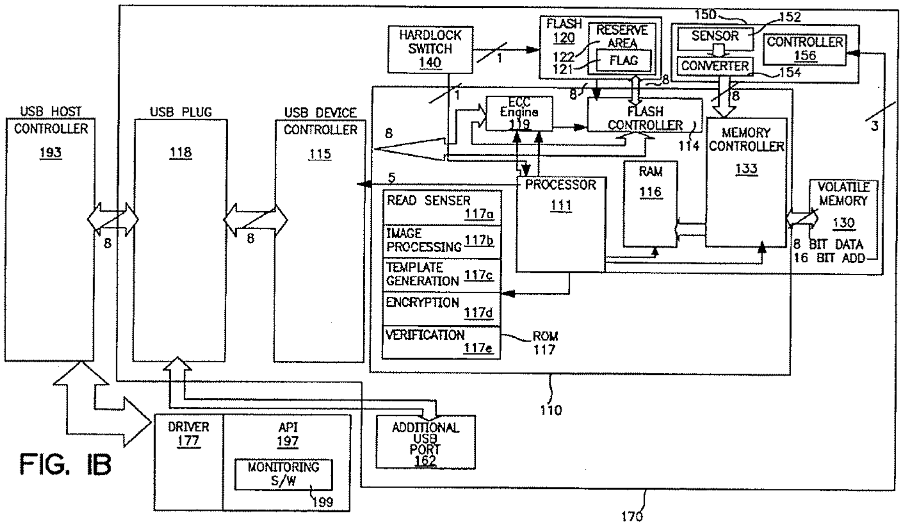


FIG. IB

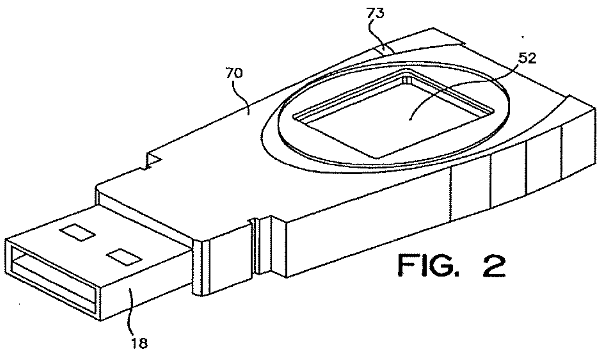


FIG. 2

Appellants' Patent Application, Figures 1B and 2

Portable device 70 is used to implement a biometrics-based authentication for controlling access to user data stored on the device. Non-volatile memory 117 stores firmware such as firmware 117a for reading fingerprint sensor 152, firmware 117b for processing fingerprint images, firmware 117c for generating templates, firmware 117d for encrypting fingerprint images and/or templates, and firmware 117e for verifying fingerprint authenticity. *See* Specification page 8, lines 30-33. Upon its first use, portable device 70 guides the user through the registration process wherein the user places his or her finger on fingerprint sensor 152, located on the surface of portable device 70, and sensor 152 is read to capture an acceptable image of the fingerprint. *See* Specification page 12, lines 1-10. An encrypted template is generated based on the fingerprint image and stored into flash memory 120. *See* Specification page 12, lines 13-17. During the authentication process, another image of the user's fingerprint is taken when the user places his or her finger on sensor 152. *See* Specification page 12, lines 32 through page 13, line 1. Microbrowser 111 directs the retrieval of the registered fingerprint template from flash memory 120. *See* Specification page 13, lines 9-10. Next, verification module 12b compares the recently taken fingerprint image against the registered image. *See* Specification page 13, lines 15-17. If a match is detected, and in situations where the portable device is used as a secure storage device, the user is authenticated and granted access to the portable device. *See* Specification page 14, lines 6-10. If no match is detected, such access is denied. *See* Specification page 13, lines 22-23.

GROUNDS OF REJECTION TO BE REVIEWED

1. The rejection of claims 1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 17, 18, and 20 as unpatentable under 35 U.S.C. § 102(e) as anticipated by U.S. Patent No. 6,088,802 (hereinafter "*Bialick*").

2. The rejection of claims 6, 12, 16, 19, and 22 as unpatentable under 35 U.S.C. § 103(a) over *Bialick*.

3. The rejection of claims 3 and 9 as unpatentable under 35 U.S.C. §103(a) over *Bialick* in view of U.S. Patent No. 6,799,275 (hereinafter "*Bjorn*").

4. The rejection of claims 23 and 24 as unpatentable under 35 U.S.C. §103(a) over *Bialick* in view of U.S. Patent No. 6,385,667 (hereinafter "*Estakhri*").

ARGUMENT

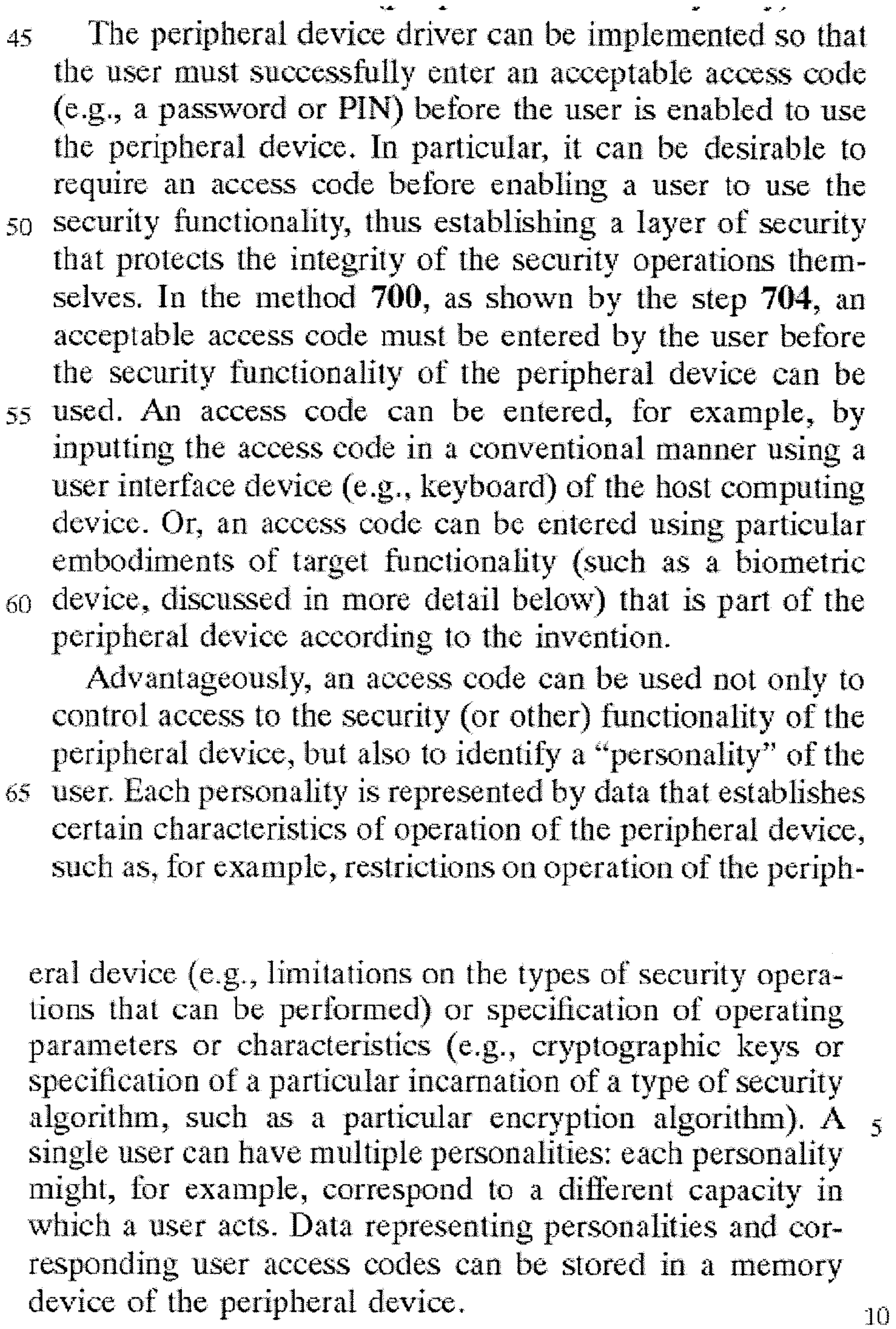
1. Rejection of claims 1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 17, 18 and 20

The Examiner rejected claims 1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 17, 18, and 20 under 35 U.S.C. § 102(e) as being anticipated by *Bialick.* Appellants respectfully traverse.

Independent claims 1, 7 and 17

In response to Appellants' prior Appeal Brief filed on October 20, 2006, the Office reopened prosecution to provide a new citation to the previously-cited *Bialick* reference. In the Office Action dated February 20, 2007, the Examiner stated that the arguments in the prior Appeal Brief were considered but are moot in view of the new grounds of rejection, including the new citation to *Bialick.* In paragraph 4 of the Office Action, the Examiner cited col. 10, line 45 – col. 11, line 10 of *Bialick* as teaching that an access code, such as a PIN, password, or biometrics, has to be entered before a user is enabled to access data stored in a memory of a peripheral device. As will be explained below, the Examiner's reliance on this portion of *Bialick* is misplaced as it does not disclose that an access code entered via a biometrics-based device can enable access to data stored in a memory of a peripheral device.

Column 10, line 45 – column 11, line 10 of *Bialick* states:



The peripheral device driver can be implemented so that the user must successfully enter an acceptable access code (e.g., a password or PIN) before the user is enabled to use the peripheral device. In particular, it can be desirable to require an access code before enabling a user to use the security functionality, thus establishing a layer of security that protects the integrity of the security operations themselves. In the method **700**, as shown by the step **704**, an acceptable access code must be entered by the user before the security functionality of the peripheral device can be used. An access code can be entered, for example, by inputting the access code in a conventional manner using a user interface device (e.g., keyboard) of the host computing device. Or, an access code can be entered using particular embodiments of target functionality (such as a biometric device, discussed in more detail below) that is part of the peripheral device according to the invention.

Advantageously, an access code can be used not only to control access to the security (or other) functionality of the peripheral device, but also to identify a "personality" of the user. Each personality is represented by data that establishes certain characteristics of operation of the peripheral device, such as, for example, restrictions on operation of the peripheral device (e.g., limitations on the types of security operations that can be performed) or specification of operating parameters or characteristics (e.g., cryptographic keys or specification of a particular incarnation of a type of security algorithm, such as a particular encryption algorithm). A single user can have multiple personalities: each personality might, for example, correspond to a different capacity in which a user acts. Data representing personalities and corresponding user access codes can be stored in a memory device of the peripheral device.

Contrary to the Examiner's assertion, this portion of *Bialick* does not disclose that an access code is required before a user is enabled to access data stored in a memory of a peripheral device. *Bialick* discloses that "it can be desirable to require an access code before enabling a user to use the *security functionality*" of the peripheral device (col. 10, lines 48-50, emphasis added), and that "an acceptable access code must be entered by the user before the *security functionality* of the peripheral device can be used" (col. 10, lines 53-55). And as Appellants show below, *Bialick* does *not* teach that storing data in a memory of the peripheral device is a security functionality. Thus requiring an access code to use a security functionality does not teach that an access code has to be entered before a user is enabled to access data stored in a non-volatile memory of a portable device.

Bialick discloses a peripheral device having two functionalities: (1) a security functionality and (2) a target functionality (col. 4, lines 55-65). *Bialick* defines a security functionality as "operations that provide one or more of the basic cryptographic functions, such as maintenance of data confidentiality, verification of data integrity, user authentication and user non-repudiation" (col. 5, lines 22-28). *Bialick* identifies the following as examples of a security functionality: cryptographic key exchange operations (col. 18, lines 1-3); hash operations (col. 18, lines 7-8); digital signature operations (col. 18, lines 12-13); key wrapping operations for symmetric and asymmetric keys (col. 18, lines 17-19); symmetric encryption operations (col. 18, lines 23-24); asymmetric (public key) encryption operations (col. 18, lines 28-30); and exponentiation operations (col. 18, lines 37-39). These examples of security functionalities all relate to performing some type of encryption on data. None of the disclosed examples of a security functionality is storing data in a non-volatile memory of a portable device, and storing data in a non-volatile memory of a portable device is not a cryptographic function. Thus, the portion of *Bialick* relied upon by the Examiner fails to teach or disclose all of the limitations of claims 1, 7, and 17.

Bialick does not disclose a mode of operation of the peripheral device in which two different target functionalities are used. *Bialick* discloses three modes that the invention can be operated in: a mode in which only the security functionality is used, a mode in which both the security functionality and the target functionality are used, and a mode in which only the target functionality is used. *See* col. 10, lines 13-18; col. 11, lines 29-30; col. 3, lines 36-40. *Bialick* does not disclose a mode in which more than one target functionality is used. Thus, *Bialick* does not disclose that an access code has to be entered before a user is enabled to access data stored in a non-volatile memory of a portable device.

Claim 1 recites that "access to the non-volatile memory is granted to a user provided that the biometrics-based authentication module authenticates the user's identity" and "access to the non-volatile memory is denied to the user otherwise." Claim 7 recites that "the microprocessor is configured to disable access to the non-volatile memory upon a determination of authentication failure by the biometrics-based authentication module." Claim 17 recites a step of "denying the user access to the non-volatile memory provided that a match is not identified." These claim limitations require a denial of user access to a non-volatile memory of a portable device when a biometrics-based authentication fails.

As set forth above, the disclosure in *Bialick* relied on by the Examiner fails to disclose using a portable device with biometrics-based authentication capability to control access to a non-volatile memory in the portable device itself. Further, *Bialick* teaches that an access code can be required to use a *security functionality* of the peripheral device, and *Bialick* teaches that storing data in a memory of the peripheral device is a target functionality, not a security functionality. *Bialick* does not disclose all of the limitations of claims 1, 7, and 17. Thus claims 1, 7, and 17 are not anticipated by *Bialick* and are in condition for allowance.

Claim 1 also recites a microprocessor and that the "biometrics-based authentication module . . . [is] controlled by the microprocessor." Claim 7 also recites a microprocessor and that the "biometrics-based authentication module . . . [is] under the control of the microprocessor." *Bialick* does not disclose a microprocessor that controls a biometrics-based authentication module. The Examiner cites to the cryptographic processing device 801 of *Bialick* as teaching the claimed microprocessor. But the cryptographic processing device 801 of *Bialick* is a special-purpose processor for performing cryptographic operations (col. 15, lines 63-67). A biometrics-based user authentication is not a cryptographic operation. *Bialick* discloses several examples of cryptographic operations, none of which is a biometrics-based user authentication. *See* col. 17, line 52 – col. 18, line 36. Further, *Bialick* identifies a cryptographic operation as a security functionality (col. 17, lines 52-60). Thus, *Bialick* does not disclose a microprocessor that controls a biometrics-based authentication module. Since *Bialick* does not disclose the claimed microprocessor, claims 1 and 7 are not anticipated by *Bialick*.

Claim 7 recites "the microprocessor is configured to disable access to the non-volatile memory upon a determination of authentication failure by the biometrics-based authentication module." As set forth above regarding claim 1, *Bialick* discloses a cryptographic processing device 801 that performs cryptographic operations. *Bialick* does not disclose that the cryptographic processing device 801 is configured to disable access to a non-volatile memory upon determination of an authentication failure by a biometrics-based authentication module. *Bialick* does not disclose all of the limitations of claim 7, thus claim 7 is in condition for allowance.

Dependent claims 2, 4, 5, 8, 10, 11, 13, 14, 18, and 20

Claims 2, 4, 5, 8, 10, 11, 13, 14, 18, and 20 depend from one of independent claims 1, 7 and 17, and are therefore allowable for at least the same reasons.

In addition, claim 4 recites the biometrics-based authentication module being comprised of a biometrics sensor fitted on one surface of the portable device. Claim 10 recites that the biometrics-based authentication module is structurally integrated with the portable device in a unitary construction. The Examiner cites col. 14, lines 48-49 and col. 14, line 59 – col. 15, line 7 of *Bialick* as teaching a biometrics sensor fitted on one surface of the portable device and structurally integrated with the portable device in a unitary construction. Appellants respectfully disagree and point out that *Bialick* merely discloses that the sensor is "positioned" on a portion of a PCMCIA card (col. 14, lines 62-64). *Bialick* does not disclose a biometrics sensor being fitted on one surface of a portable device or a biometrics-based authentication module being structurally integrated with a portable device in a unitary construction. For these additional reasons, claims 4 and 10 are not anticipated by *Bialick* and are in condition for allowance.

Claims 5 and 11 recite the non-volatile memory comprising flash memory. The Examiner cites Figure 8, item 803 and col. 16, lines 10-11 of *Bialick* as disclosing the use of non-volatile memory, including flash memory. As set forth above regarding claims 1, 7, and 17, *Bialick* does not disclose such memory in the context of biometrics-based authentication used to grant or deny user access to data stored in the peripheral device. For these additional reasons, claims 5 and 15 are not anticipated by *Bialick* and are in condition for allowance.

Claim 13 recites the microprocessor being configured to direct the biometrics-based authentication module to capture and store the first biometrics marker provided that no biometrics marker has been stored in the non-volatile memory. The Examiner cites col. 14, lines 55-58 of *Bialick* as disclosing this limitation. However, as set forth above regarding claim 7, *Bialick* does not disclose a microprocessor that controls a biometrics-based authentication module. *Bialick* also does not disclose a microprocessor that is configured to direct a biometrics-based authentication module to capture and store a first biometrics marker. For these additional reasons, claim 13 is not anticipated by *Bialick* and is in condition for allowance.

Claim 14 recites the microprocessor being configured to enable access to the non-volatile memory upon a determination of authentication success by the biometrics-based authentication module. The Examiner cites col. 10, line 45 – col. 11, line 10; col. 14, line 10 – col. 15, line 23; and col. 16, lines 10-16 of *Bialick* as disclosing this limitation. As set forth above regarding claim 7, *Bialick* does not disclose a microprocessor that controls a biometrics-based authentication module. *Bialick* also does not disclose a microprocessor configured to enable access to a non-volatile memory upon determination of authentication success by a biometrics-based authentication module. For these additional reasons, claim 14 is not anticipated by *Bialick* and is in condition for allowance.

2. Rejection of claims 6, 12, 16, 19, and 22

The Examiner rejected claims 6, 12, 16, 19 and 22 under 35 U.S.C. § 103(a) as being unpatentable over *Bialick.* Appellants respectfully traverse.

Claims 6, 12, 16, 19, and 22 depend from one of claims 1, 7, and 17, and are therefore allowable for at least the same reasons.

Claims 6 and 16 recite that the "microprocessor is configured to provide a bypass mechanism for authentication upon a determination of authentication failure by the biometrics-based authentication module." Claims 6 and 16 depend from claims 1 and 7, respectively, and as set forth above, *Bialick* does not disclose the microprocessor of claims 1 and 7. *Bialick* also does not disclose a microprocessor that provides a bypass mechanism for authentication when authentication by a biometrics-based authentication module fails. The cryptographic processing device 801 of *Bialick* is not configured to provide a bypass mechanism for authentication. The Examiner has not identified any prior art reference that discloses a microprocessor that provides a bypass mechanism for authentication when a biometrics-based authentication fails.

The Examiner stated that it would have been obvious to modify *Bialick* to include a microprocessor configured to provide a bypass mechanism because "a person having ordinary skill in the art would have been motivated to do so by the suggestion provided by [*Bialick*] to use the security functionality, thus enabling a layer of security that protects the integrity of the restricted resources." Appellants respectfully disagree. Simply suggesting use of a security functionality does not teach or suggest use of a bypass mechanism for authentication when a biometrics-based authentication module fails. Appellants' specification identifies an example of a situation in which the claimed bypass mechanism can be used: a malfunction of verification module 12b. In the event of a biometrics-based authentication module malfunction, the bypass mechanism can enable an authorized user to gain access to the data stored in the memory of the portable device until the module is repaired. *See* specification, pp. 13-14. *Bialick* identifies no such situation, and does not teach or suggest that there is any need to deal with a malfunction of a biometrics-based authentication. *Bialick* does not teach or suggest using an additional user authentication mechanism when a biometrics-based authentication fails. Thus claims 6 and 16 are not obvious in view of *Bialick* and are in condition for allowance.

Claim 22 recites a step of "providing the user with a bypass authentication procedure provided that a match is not identified." The Examiner stated that it would have been obvious to modify *Bialick* to include a step of providing a bypass authentication procedure provided that a match is not identified because "a person having ordinary skill in the art would have been motivated to do so by the suggestion provided by [*Bialick*] to use the security functionality, thus enabling a layer of security that protects the integrity of the restricted resources." Appellants respectfully disagree. Simply suggesting use of a security functionality does not teach or suggest use of a bypass authentication when a match between biometrics markers is not identified. Appellants' specification identifies an example of a situation in which the claimed bypass mechanism can be used: a malfunction of verification module 12b. In the event of a biometrics-based authentication module malfunction, the bypass mechanism can enable an authorized user to gain access to the data stored in the memory of the portable device until the module is repaired. *See* specification, pp. 13-

14. *Bialick* identifies no such situation, and does not teach or suggest that there is any need to deal with a failure of a biometrics-based authentication. There is no teaching or suggestion in *Bialick* of using an additional authentication procedure when a match between biometrics markers is not identified. Thus claim 22 is not obvious in view of *Bialick* and is in condition for allowance.

Claim 12 recites that "the biometrics-based authentication module is further configured to encrypt the first biometrics marker before storing the first biometrics marker in the non-volatile memory." The Examiner stated that it would have been obvious to one of ordinary skill in the art to modify *Bialick* to include encrypting a first biometrics marker before storing the first biometrics marker in a non-volatile memory, and that *Bialick* provides a suggestion to enhance the security of a biometrics-based access control method. Appellants respectfully disagree. *Bialick* does not teach or suggest performing any type of security functionality, such as a cryptographic operation, on a biometrics marker that is to be stored in a non-volatile memory of a peripheral device. *Bialick* teaches that a cryptographic operation is a security functionality that is separate from any target functionality. There is no teaching or suggestion in *Bialick* to modify a biometrics-based authentication to encrypt a first biometrics marker before storing the first biometrics marker in the non-volatile memory of a portable device. Thus claim 12 is not obvious in view of *Bialick* and is in condition for allowance.

Claim 19 recites that "the registered biometrics marker is stored in an encrypted format." The Examiner stated that it would have been obvious to one of ordinary skill in the art to modify *Bialick* to include storing a registered biometrics marker in an encrypted format, and that *Bialick* provides a suggestion to enhance the security of a biometrics-based access control method. Appellants respectfully disagree. *Bialick* does not teach or suggest performing any type of security function, such as a cryptographic operation, on a registered biometrics marker that is stored in a non-volatile memory of a peripheral device. *Bialick* teaches that a cryptographic operation is a security functionality that is separate from any target functionality. There is no teaching or suggestion in *Bialick* to modify a target functionality of biometrics-based authentication to store a registered biometrics marker in an encrypted format. Thus claim 19 is not obvious in view of *Bialick* and is in condition for allowance.

3. Rejection of claims 3 and 9

The Examiner rejected claims 3 and 9 under 35 U.S.C. § 103(a) as being unpatentable over *Bialick* in view of *Bjorn*. Appellants respectfully traverse.

Claims 3 and 9 depend from claims 1 and 7, respectively, and are therefore allowable for at least the same reasons. Further, claims 3 and 9 are allowable over *Bialick* in view of *Bjorn* because these references, either alone or in combination, do not teach or disclose all the limitations of claims 3 and 9.

Claim 3 recites a "USB plug for coupling the portable device directly to a USB socket of another USB-compliant device." The Examiner stated that *Bialick* does not disclose this limitation, but that *Bjorn* teaches a device with a data bus that conforms to a USB standard (col. 2, lines 59 and 60) and that it would have been obvious to combine *Bjorn* with *Bialick* because *Bjorn* teaches that the USB standard provides for faster transfer of a digitized image. But the discussion in *Bjorn* about a device having a bus conforming to a USB standard that can receive digital images does not teach or suggest a portable device that has a USB connector that enables the portable device to be coupled directly to a USB socket of another USB-compliant device. *Bjorn* teaches coupling peripheral devices such as a display, a keyboard, and a mouse to a computer system that has a USB bus (col. 2, line 64 – col. 3, line 10), but does not teach or suggest *directly coupling* a USB plug of a portable device having a non-volatile memory to a USB socket of a USB-compliant device. The memory device of *Bjorn* is a smart card that has a size and shape similar to a plastic credit card (col. 1, lines 16-18), a form that physically cannot support a USB plug, and *Bjorn* does not disclose coupling a smart card directly to a USB socket of a USB-compliant device. Thus *Bjorn* does not teach or disclose the limitation recited in claim 3.

Claim 9 recites a "USB device controller coupled to the bus and a USB plug coupled to the bus, such that the portable device is capable of being coupled directly to a USB socket of . . . a host platform." The Examiner stated that *Bialick* does not disclose this limitation, but that *Bjorn* teaches a device with a data bus that conforms to a USB standard (col. 2, lines 59 and 60) and that it would have been obvious to combine *Bjorn* with *Bialick* because *Bjorn* teaches that the USB standard provides for faster transfer of a digitized image. But as set forth above regarding claim 3, *Bjorn* does not disclose a portable device that has a USB connector that enables the portable device to be coupled directly to a USB socket of another USB-compliant device. Further, *Bjorn* does not disclose a portable device that has a USB plug coupled to a bus of the portable device. *Bjorn* teaches coupling peripheral devices such as a display, a keyboard, and a mouse to a computer system that has a USB bus (col. 2, line 64 – col. 3, line 10), but does not teach or suggest *directly coupling* a USB plug of a portable device having a non-volatile memory to a USB socket of a USB-compliant device. The memory device of *Bjorn* is a smart card that has a size and shape similar to a plastic credit card (col. 1, lines 16-18), a form that physically cannot support a USB plug, and *Bjorn* does not disclose coupling a smart card directly to a USB socket of a USB-compliant device. Also, *Bjorn* discloses a computer system having a bus, and does not disclose a portable device that has a bus. Thus *Bjorn* does not teach or disclose the limitation recited in claim 9.

Bialick and *Bjorn,* either alone or in combination, do not teach or suggest all of the limitations of claims 3 and 9. Thus claims 3 and 9 are not obvious in view of the cited references and are in condition for allowance.

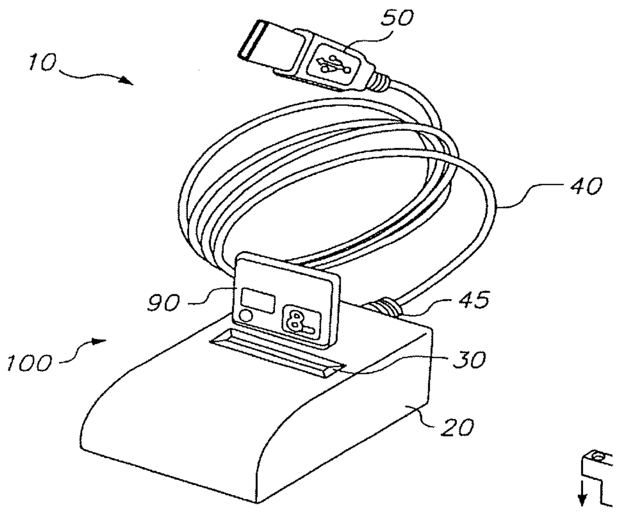
4. Rejection of claims 23 and 24

The Examiner rejected claims 23 and 24 under 35 U.S.C. § 103(a) as being unpatentable over *Bialick* in view of *Estakhri.* Appellants respectfully traverse.

Claim 23 recites a "fingerprint module" and a "memory . . . configured to store at least one fingerprint template as well as user data." As set forth above regarding claims 1, 7, and 17, *Bialick* discloses that biometrics-based authentication can be used to enter an access code before enabling use of a *security functionality*. *Bialick* does not disclose that a fingerprint module can be used to enter an access code to enable storing user data in a memory of a portable device. Thus *Bialick* does not disclose a portable device having both a fingerprint module and a memory configured to store user data.

Claim 23 also recites "a memory controller . . . coupled to the memory . . . [for] controlling access to the memory." The Examiner states that the cryptographic processing device 801 of *Bialick* discloses the memory controller of claim 23. But as set forth above regarding claims 1, 7, and 17, the cryptographic processing device 801 of *Bialick* is a special-purpose processor for performing cryptographic operations (col. 15, lines 63-67). *Bialick* identifies cryptographic operations as security functionalities, and none of the examples of security functionalities provided by *Bialick* encompass controlling access to a memory. Thus *Bialick* does not disclose the memory controller recited in claim 23.

Claim 23 also recites "a USB plug integrated into the housing without an intervening cable and capable of coupling the unitary portable storage device directly to a USB socket on a host computer." The Examiner stated that *Estakhri* teaches this limitation. But *Estakhri* does not teach a USB plug integrated into the housing of a portable memory device without an intervening cable. Rather, *Estakhri* teaches an interface system that has a 50-pin connection as a second end 315 for connection to a removable memory card and has a first end 314 to couple the interface system to a host computer (col. 5, lines 18-44). *Estakhri* merely teaches that the first end 314 of the interface system is configured for coupling to a host computer system 330 (col. 5, lines 18-20, 45-47), but does not disclose how this coupling is achieved. The first end 314 is for coupling the *interface system* to a host computer, not for coupling a portable storage device to a host computer. In a prior art embodiment where an interface system supports a USB plug, *Estakhri* discloses that the USB plug 50 is connected to the housing 20 via a *cable 40*, as clearly shown in Figure 1A of *Estakhri*, reproduced below. The removable memory card of *Estakhri* has a 50-pin connection, and does not have a USB plug integrated into its housing. *Estakhri* does not teach or disclose a USB plug that is integrated into the housing of a portable data storage device without an intervening cable as recited in claim 23 and as shown in Figure 2 of Appellants' application, reproduced below.



***Estakhri*, Figure 1A**

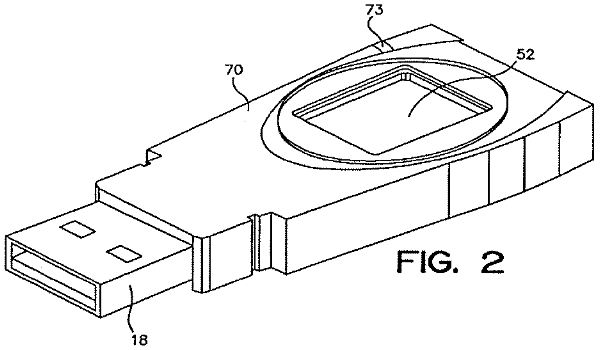


FIG. 2

Appellants' Patent Application, Figure 2

It would not have been obvious to a skilled artisan at the time of the invention to combine *Bialick* and *Estakhri* because the combination of *Bialick* and *Estakhri* does not disclose all of the limitations of claim 23, and the two references disclose systems geared towards completely opposite objectives. *Bialick* teaches an access control system that serves to restrict access to information stored in a host computer, whereas *Estakhri* teaches an interfacing system that facilitates access to information stored in multiple memory cards. Thus, *Bialick* and *Estakhri* teach two distinct endeavors that seek to achieve opposite results: restricting access to stored information in a host computer versus facilitating access to stored information in multiple memory devices. The fact that *Bialick* and *Estakhri* refer to flash memory and *Estakhri* refers to the USB protocol does not, without more, make the two references combinable, and the combination of the two references does not disclose all of the limitations of claim 23. As a result, a skilled artisan would not seek to combine the teachings in *Bialick* and *Estakhri.*

Bialick and *Estakhri*, either alone or in combination, do not teach or disclose all of the limitations of claim 23. Claim 23 is not obvious in view of the cited references and is in condition for allowance.

Claim 24 depends from claim 23, and is allowable for at least the same reasons. Further, claim 24 recites that "at least a portion of the USB plug protrudes from the housing to facilitate direct coupling of the unitary portable storage device to the USB socket." The Examiner stated that *Estakhri* discloses this limitation. But as set forth above regarding claim 23, *Estakhri* does not disclose a USB plug integrated into the housing of a portable storage device, so *Estakhri* cannot disclose that at least a portion of a USB plug integrated into the housing of a portable storage device protrudes from the housing. *Bialick* and *Estakhri*, either alone or in combination, do not disclose all of the limitations of claim 24. Claim 24 is not obvious in view of the cited references and is in condition for allowance.

CONCLUSION

For the foregoing reasons, Appellants respectfully submit that the pending claims are not anticipated or obvious in view of the cited references and are in condition for allowance.

Respectfully submitted,

Dated: March 20, 2008

Warren S. Heit (Reg. No. 36,828)
WHITE & CASE LLP
1155 Avenue of the Americas
New York, NY 10036
(650) 213-0321

APPENDIX A: CLAIMS APPENDIX

1. (previously presented) A portable device comprising:

a microprocessor;

a non-volatile memory coupled to the microprocessor; and

a biometrics-based authentication module coupled to and controlled by the microprocessor, wherein access to the non-volatile memory is granted to a user provided that the biometrics-based authentication module authenticates the user's identity and wherein access to the non-volatile memory is denied to the user otherwise.

2. (previously presented) The portable device as recited in Claim 1 wherein the biometrics-based authentication module is a fingerprint authentication module.

3. (previously presented) The portable device as recited in Claim 1 further comprising a universal serial bus (USB) plug for coupling the portable device directly to a USB socket of another USB-compliant device.

4. (previously presented) The portable device as recited in Claim 1 wherein the biometrics-based authentication module comprises a biometrics sensor fitted on one surface of the portable device.

5. (previously presented) The portable device as recited in Claim 1 wherein the non-volatile memory comprises flash memory.

6. (previously presented) The portable device as recited in Claim 1 wherein the microprocessor is configured to provide a bypass mechanism for authentication upon

a determination of authentication failure by the biometrics-based authentication module.

7. (previously presented) A portable device comprising:

a bus;

a microprocessor coupled to the bus;

a non-volatile memory coupled to the bus; and

a biometrics-based authentication module coupled to the bus, wherein under the control of the microprocessor the biometrics-based authentication module is configured to (1) capture a first biometrics marker; (2) store the first biometrics marker in the non-volatile memory; (3) capture a second biometrics marker; and (4) determine whether the second biometrics marker can be authenticated against the first biometrics marker; and wherein the microprocessor is configured to disable access to the non-volatile memory upon a determination of authentication failure by the biometrics-based authentication module.

8. (previously presented) The portable device as recited in Claim 7 wherein the biometrics-based authentication module is a fingerprint authentication module.

9. (previously presented) The portable device as recited in Claim 7 further comprising a universal serial bus (USB) device controller coupled to the bus and a USB plug coupled to the bus, such that the portable device is capable of being coupled directly to a USB socket of and communicating with a host platform via the USB plug.

10. (previously presented) The portable device as recited in Claim 7 wherein the biometrics-based authentication module is structurally integrated with the portable device in a unitary construction and comprises a biometrics sensor being disposed on one surface of the portable device.

11. (previously presented) The portable device as recited in Claim 7 wherein the non-volatile memory comprises flash memory.

12. (previously presented) The portable device as recited in Claim 7 wherein the biometrics-based authentication module is further configured to encrypt the first biometrics marker before storing the first biometrics marker in the non-volatile memory.

13. (previously presented) The portable device as recited in Claim 7 wherein the microprocessor is configured to direct the biometrics-based authentication module to capture and store the first biometrics marker provided that no biometrics marker has been stored in the non-volatile memory.

14. (previously presented) The portable device as recited in Claim 7 wherein the microprocessor is configured to enable access to the non-volatile memory upon a determination of authentication success by the biometrics-based authentication module.

15. (cancelled)

16. (previously presented) The portable device as recited in Claim 7 wherein the microprocessor is configured to provide a bypass mechanism for authentication upon a determination of authentication failure by the biometrics-based authentication module.

17. (previously presented) A biometrics-based authentication method implemented using a portable device, the method comprising the steps of:

(a) obtaining a first biometrics marker from a user with a biometrics sensor installed on the portable device;

(b) retrieving a registered biometrics marker from a non-volatile memory of the portable device, the registered biometrics marker having been stored therein during a registration process;

(c) comparing the first biometrics marker against the registered biometrics marker;

(d) denying the user access to the non-volatile memory provided that a match is not identified in said step (c); and

(e) signaling an authentication success provided that a match is identified in said step (c).

18. (previously presented) The biometrics-based authentication method as recited in Claim 17 wherein the registered biometrics marker is a fingerprint.

19. (previously presented) The biometrics-based authentication method as recited in Claim 17 wherein the registered biometrics marker is stored in an encrypted format.

20. (previously presented) The biometrics-based authentication method as recited in Claim 17 wherein said step (d) comprises granting the user access to the non-volatile memory.

21. (cancelled)

22. (previously presented) The biometrics-based authentication method as recited in Claim 17 further comprising the step of providing the user with a bypass authentication procedure provided that a match is not identified in said step (c).

23. (previously presented) A unitary portable data storage device having biometrics capability which can be directly plugged into a universal serial bus (USB) socket of a host computer, the device comprising:

a housing;

a fingerprint module, at least a portion of which is housed within the housing, the fingerprint module including a sensor disposed on an exterior surface of the housing;

a memory including non-volatile memory, the memory housed within the housing and coupled to the fingerprint module and is configured to store at least one fingerprint template as well as user data;

a memory controller housed within the housing and coupled to the memory, the memory controller controlling access to the memory;

a USB plug integrated into the housing without an intervening cable and capable of coupling the unitary portable data storage device directly to a USB socket on a host computer; and a USB device controller housed within the housing, the USB device controller enabling the unitary portable data storage device to communicate with the host computer via the USB protocol;

wherein the fingerprint module is configured to (1) receive a fingerprint sample from a user placing a finger on the sensor; (2) compare the fingerprint sample with said at least one fingerprint template; and (3) reject a request from the user to access the user data stored in the memory provided that the comparison in said step (2) results in no match.

24. (previously presented) The unitary portable data storage device as recited in Claim 23 wherein at least a portion of the USB plug protrudes from the housing to facilitate direct coupling of the unitary portable data storage device to the USB socket of a computer.

APPENDIX B: EVIDENCE APPENDIX

NONE

APPENDIX C: RELATED PROCEEDINGS APPENDIX

NONE